

## CHAPTER 17 ELECTRONIC COMMERCE

### MULTIPLE CHOICE

1. Which of the following statements is TRUE?
- electronic commerce encourages international business transactions
  - technology allows contracts to be performed more quickly
  - technology reduces marketing costs
  - the law governing electronic commerce is uncertain
  - all of the above

Answer: e      Difficulty: 1      Page: 375      Skill Type: recall

2. Rolf Dog Food has decided to implement an electronic commerce initiative. Although Rolf has only announced its policy to its larger trading partners, the company has also begun allowing for electronic mail from customers through its web site. In turn, it has responded electronically. Recently, one its customers sent the company an email canceling her regular monthly order. Rolf decided not to recognize the message on the basis of its electronic format, without notification to the sender. According to the *Uniform Electronic Commerce Act* which of the following statements is TRUE?

- Rolf is justified in refusing to recognize the electronic message
- Rolf may either accept or refuse the message at will
- Rolf might be said to have consented to the use of electronic documents and, if so, must accept the customer's message
- Rolf must fill the customer's order
- none of the above

Answer: c      Difficulty: 3      Page: 376      Skill Type: applied

3. Which of the following correctly illustrates the *functional equivalence* for a legal signature?

- attaching an electronic signature to an electronic document
- signing your full name on a standard form
- clicking "I Accept" in a dialogue box in a clickwrap agreement
- writing your name on the bottom of a hand written agreement
- all of the above

Answer: e      Difficulty: 2      Page: 376      Skill Type: applied

4. Eta sends Morley a contractual offer via email from her Calgary office. The email contains a provision indicating that the offer expires at 5:00 PM, Calgary time. Morley replies to Eta's offer from his Vancouver office, indicating that he accepts her offer. Morey's email leaves his control at 4:52 PM (Vancouver time) and reaches an information system within Eta's control instantaneously. Eta waited in her office till 5:10 PM (Calgary time), but received nothing (because of the one hour time difference between Vancouver and Calgary). The next day, when Eta found Morley's email in her

inbox (time stamped @ 5:52 Calgary time), she phoned Morley to refuse the deal.

According to the *Uniform Electronic Commerce Act*, which of the following is TRUE?

- a. Eta and Morley have definitely concluded a binding agreement, which was formed at 5:52 Calgary time
- b. Eta and Morley have definitely concluded a binding agreement, which was formed at 4:52 Calgary time
- c. Eta's offer expired
- d. Morley accepted Eta's offer, but the contract did not come into affect until the next morning when Eta opened her email
- e. once she opened her email it was too late for Eta to refuse the deal

Answer: c     Difficulty: 3     Page: 377     Skill Type: applied

5. After becoming tired of the muzzak piped into your office, you decide to subscribe to an online, listener-supported radio station dedicated to jazz and blues music. You had thought that there is no upfront fee, but that listeners may make a donation using their electronic wallets. Clicking through the site, you are asked to provide certain information on a contractual form. One day, after several visits to the web site, you notice a hyperlink labeled *terms of service* while viewing the previous hour's play list. You click the link and a document opens, indicating that, by streaming music from the web site, you have agreed to pay a flat fee on a monthly basis with a minimum subscription of one year. On your previous visits, you never noticed the hyperlink, which is barely visible in fine print, at the bottom corner of the home page right next to a flashy and distracting animation. Which of the following BEST characterizes this situation?

- a. you have entered into a webwrap contract and owe a year of monthly fees
- b. you have entered into a clickwrap contract and owe a year of monthly fees
- c. you have entered into a shrinkwrap contract and owe a year of monthly fees
- d. you have not entered into a contract
- e. you may have entered into a contract but its terms likely do not include a year of monthly fees.

Answer: e     Difficulty: 3     Page: 378     Skill Type: applied

6. Which of the following propositions is supported by the decision in *Rudder v Microsoft*?

- a. the fact that a party clicked "I AGREE" without actually reading the terms of the agreement will render it unenforceable
- b. the fact that a party clicked "I AGREE" without actually reading the terms of the agreement will NOT render the contract unenforceable
- c. clicking "I AGREE" is not a legally permissible means of communicating acceptance of a contractual offer
- d. clicking "I AGREE" is ineffectual unless there is a printout of the agreement to satisfy the parol evidence rule
- e. none of the above

Answer: b     Difficulty: 2     Page: 379     Skill Type: recall

7. Which of the following would best explain why certain terms in an online agreement might be found to be of NO LEGAL EFFECT?
- the terms are boilerplate provisions
  - the terms are displayed in red font, rather than black
  - the terms cannot be stored electronically
  - the terms are not accessible to the customer until after the transaction is complete
  - none of the above

Answer: d    Difficulty: 2    Page: 378    Skill Type: applied

8. Which of the following would be legally recognized pursuant to the *Uniform Electronic Commerce Act*?
- purchasing an item from a web site with your credit card by clicking through a series of dialogue boxes
  - programming your shopping bot (an automated electronic device) to purchase an item from a web site with your credit card
  - ordering an item online through another person's shopping bot
  - programming your shopping bot to purchase an item from another person's shopping bot
  - all of the above

Answer: e    Difficulty: 2    Page: 380    Skill Type: applied

9. Bread and Butter Inc has decided to begin retailing its products over the internet. It is particularly worried that errors generated by its automated computer system may result in filling under-priced orders. The company has retained you for advice on this issue. Accordingly, you will advise them to design their web site so that
- it creates invitations to treat.
  - it extends offers to purchase.
  - it encourages customers to accept offers only after reading all terms and conditions.
  - it eliminates consideration.
  - none of the above

Answer: a    Difficulty: 1    Page: 380    Skill Type: applied

10. The International Widget Co has approached you seeking advice. It is currently embroiled in a dispute with one of its regular trading partners. As a result of spilling Orange Crush on his keyboard, the trading partner's Purchasing Officer accidentally ordered 700 widgets, instead of the usual monthly 70. Figuring that the extraordinary order would not be processed, he did not bother informing International Widget about the mistake. Relying on the accuracy of the order, International Widgets bought supplies necessary to make 700 widgets. The trading partner refuses to carry out the transaction.

Assuming the relevant jurisdiction follows the approach adopted by the *Uniform Electronic Commerce Act*, which of the following is most likely TRUE?

- a. International Widget's trading partner will not be bound by the order
- b. International Widget's trading partner will be bound by the order
- c. International Widget can recover from its trading partner the cost of no more than 350 widgets
- d. International Widget can recover from its trading partner the cost of no more than 500 widgets
- e. none of the above

Answer: b    Difficulty: 2    Page: 381    Skill Type: applied

11. Which of the following may serve an *authenticating function* with respect to electronic documents?

- a. an electronic signature
- b. a certification authority
- c. public key infrastructure
- d. cryptography
- e. all of the above

Answer: e    Difficulty: 1    Page: 381    Skill Type: recall

12. Which of the following is used to verify the identity of the person purporting to provide an electronic signature?

- a. file formatting
- b. a digital certificate
- c. a court order
- d. information security
- e. digital watermarking

Answer: b    Difficulty: 2    Page: 381    Skill Type: recall

13. When you arrived at work this morning, there was a memo on your desk asking you to draft a report that outlines how a public key infrastructure might be implemented in the company's business practices. Although you know that PKI can be used for both encrypting messages and verifying electronic signatures, you are confused as to their respective purposes. After conducting further research, which of the following will you find to be TRUE?

- a. decrypting a message requires the sender to use her public key, while verifying her electronic signature requires the recipient to use his private key
- b. decrypting a message requires the recipient to use her private key, while verifying her electronic signature requires the use of her public key
- c. decrypting a message requires the sender to use her private key, while verifying her electronic signature requires the use of her public key

- d. decrypting a message requires the recipient to use her public key, while verifying her electronic signature requires the use of her private key
- e. decrypting and encryption are one and the same

Answer: b    Difficulty: 3    Page: 382    Skill Type: applied

14. Which of the following security threats may be achieved by an online intruder?
- a. dilution of corporate brands
  - b. causing system failures
  - c. stealing information-based assets
  - d. scaring off customers
  - e. all of the above

Answer: e    Difficulty: 1    Page: 383    Skill Type: recall

15. After your company's web site is defaced by a hacker, you are assigned the task of creating a policy aimed at avoiding similar attacks in the future. Because it has been determined that the attack was internal, you have chosen to focus on deterring company employees from such behaviour. Which of the following issues will you be sure to include in the policy in order to achieve your goal?
- a. use of confidential information
  - b. email use
  - c. computer mischief
  - d. monitoring employee communications
  - e. intercepting employee communications

Answer: c    Difficulty: 2    Page: 385    Skill Type: applied

16. After reading an article about domain name related entrepreneurship, you decide to register several domain names for resale. Subsequently, you receive a complaint alleging that you have registered one of those names in bad faith. The complainant has filed for arbitration. The name in question is breadandbutter.com. The complainant, Domain Acquisitions Co, does not hold a registered trademark in the name nor do they conduct business under the name. As far as you can tell, no one is currently operating under this name. Based on these facts, which of the following statements is TRUE?
- a. you have an intellectual property right in the name
  - b. you are a cybersquatter
  - c. the complainant can claim the *good faith* justification
  - d. your domain name dispute cannot be litigated in court
  - e. all of the above

Answer: b    Difficulty: 3    Page: 386    Skill Type: applied

17. Which of the following propositions is supported by the decision in *Wal-Mart Stores Inc v wallmartsucks.com and Kenneth J Harvey*?
- a. Wal-Mart sucks
  - b. the domain name dispute process should be expanded

- c. arbitration provides a general remedy for all damages related to domain names
- d. corporate criticism constitutes a legitimate interest in a domain name
- e. the suffix *sucks* does not prevent a domain name from being confusingly similar

Answer: d    Difficulty: 2    Page: 387    Skill Type: applied

18. Which of the following tests is irrelevant to a determination of the appropriate jurisdiction for litigation arising from online interaction?
- a. whether there is a real and substantial connection to the place where jurisdiction is being sought
  - b. whether the web site has an actual impact in the place where jurisdiction is being sought
  - c. whether the defendant is culpable
  - d. whether the web site merely posts information, or requires customers to interact
  - e. none of the above are irrelevant

Answer: a    Difficulty: 1    Page: 388    Skill Type: recall

19. Which of the following propositions is supported by the decision in *Alteen v Informix Corp*?
- a. the availability of web site information to Canadian citizens is sufficient to establish jurisdiction
  - b. the availability of web site information to Canadian citizens is NOT sufficient to establish jurisdiction
  - c. jurisdiction is dependent on the commercial nature of the information made available
  - d. Canadian courts have no jurisdiction over online business activities
  - e. none of the above

Answer: a    Difficulty: 2    Page: 388    Skill Type: recall

20. RAS Auto Parts, a Canadian company, recently received some decidedly unfavourable publicity stemming from an incident that took place at a Caribbean conference attended by its board of directors. The story was published in the *Trinidad Daily Online*. RAS would like to bring a defamation suit against the *Daily Online* in Canada. In order to obtain jurisdiction in Canada, under the *effects-based approach*, which of the following elements must RAS prove?
- a. how the harm was suffered
  - b. why the harm was suffered
  - c. where the harm was suffered
  - d. what harm was done
  - e. all of the above

Answer: c    Difficulty: 2    Page: 389    Skill Type: applied

21. Mike Internet Inc offers an internet connection and an email account for \$9 per month. The company does not retail goods, nor does it provide a forum for subscriber auctions. The company will not disclose personal information about its customers unless required to do so by law. Which of the following is most likely TRUE?

- a. Mike is an internet access provider
- b. Mike is an online service provider
- c. Mike is an online intermediary
- d. Mike is unlikely to be seen as a publisher of its customers' communications
- e. all of the above

Answer: e      Difficulty: 1      Page: 391      Skill Type: applied

22. Syntax Systems has launched a new electronic newsletter. Similar to the use of a listserv, the newsletter is composed of subscriber submissions (rather than content generated by the news service itself). Each day's accumulated subscriber submissions are automatically packaged and automatically sent by mass email without editorial review. (In fact, the whole point of the newsletter is that no one knows what anyone else will say until it is disseminated.) Revenue for the newsletter is generated through advertising. Like the rest of the process, the advertising is automated: an advertising bot searches the subscriber threads for keywords in order to tailor the advertising to the topics of discussion and thereby support premium rates. If the US approach set out in *Cubby* and *Stratton-Oakmont* is adopted, which of the following is TRUE?

- a. Syntax is likely to be liable in the event that an illegal message was posted
- b. Syntax is unlikely to be liable in the event that an illegal message was posted
- c. Syntax is exempted from liability by virtue of being an internet access provider
- d. Syntax can only avoid liability if it attempts to censor illegal messages
- e. none of the above

Answer: b      Difficulty: 3      Page: 392      Skill Type: applied

23. Which of the following kinds of online behaviour might potentially attract liability?

- a. posting a defamatory remark
- b. distributing materials subject to copyright
- c. disclosing personal information
- d. trademark infringement
- e. all of the above

Answer: e      Difficulty: 1      Page: 391      Skill Type: applied

24. According to current policy, which of the following online intermediaries is least likely to be liable for carrying defamatory content?
- The National Post Online
  - CNN.com
  - University of Toronto Libraries Online
  - CBC.ca
  - Canwestglobal.com

Answer: c    Difficulty: 2    Page: 392    Skill Type: applied

25. Which of the following activities is typical of a *dot con*?
- multi-level marketing
  - an online auction
  - electronic contracting
  - banner advertising
  - all of the above

Answer: a    Difficulty: 2    Page: 393    Skill Type: recall

26. You have recently gone into business as a consultant, specializing in the area of online consumer protection. As part of your services, you offer a seminar on how to avoid fraudulent transactions. Which of the following practices will you immediately suggest to your clients?
- transacting as a mere conduit
  - adopting authentication procedures
  - utilizing an open-access network
  - implementing electronic contracting and instantaneous communication
  - all of the above

Answer: b    Difficulty: 2    Page: 394    Skill Type: applied

27. You have recently gone into business as a consultant, specializing in the area of online consumer protection. As part of your services, you offer a seminar on how to avoid online consumer complaints. Which of the following practices will you immediately suggest to your clients?
- be sure your online contracts include extensive use of specialized legal terminology
  - weave promotional materials into the terms and conditions of sale
  - be sure to accurately describe all online goods and services
  - dispense with confirmation procedures
  - promise not to collect any personal information.

Answer: c    Difficulty: 3    Page: 394    Skill Type: applied



28. Which of the following is a good reason for incurring the costs associated with implementing Industry Canada's consumer protection principles into your business?
- your business is legally required to do so
  - to avoid competition from multi-level marketers
  - to avoid the need for adopting a privacy-compliance policy
  - you will strengthen consumer confidence in your products
  - all of the above

Answer: d Difficulty: 2 Page: 395 Skill Type: applied

29. According to consumer protection principles, when should your business provide a refund for a completed transaction?
- when the purchase was in fact made by a third party stranger
  - when the transaction was the result of a keystroke error
  - when the customer has entered into the transaction without adequate information
  - when the customer mistakenly entered into the transaction and has not yet enjoyed a material benefit
  - all of the above

Answer: e Difficulty: 2 Page: 395 Skill Type: applied

30. Which of the following practices should be adopted in order to respect the consumer protection principles advocated by Industry Canada?
- sending unsolicited email only to parties who you think will be interested
  - sharing customer information only with trusted business partners
  - providing the information necessary for customers to make informed choices
  - implementing encrypted electronic payment systems
  - all of the above

Answer: c Difficulty: 3 Page: 398 Skill Type: applied

### TRUE OR FALSE

1. Canada's *Uniform Electronic Commerce Act* creates rights, powers, obligations and immunities with respect to electronic commerce-related activities within Canada.

Answer: false Difficulty: 1 Page: 375 Skill Type: recall

2. The board of directors for Scroll Networks has decided to implement the use of electronic documents in all their business practices. Although they have not explicitly announced this new policy to their business partners, they have recently begun promoting a cost-savings scheme for those partners who undertake to communicate electronically. Based on its actions, Scroll will likely be required to accept electronic documents from any of its business partners who have received the promotions and acted accordingly.

Answer: true Difficulty: 2 Page: 376 Skill Type: applied

3. The *Uniform Electronic Commerce Act* states that electronic communications are deemed sent when they leave the senders control, whether they are received or not.

Answer: true Difficulty: 2 Page: 377 Skill Type: recall

4. A web-wrap contract always occurs in the context of mass-marketed software.

Answer: false Difficulty: 2 Page: 378 Skill Type: recall

5. A digital certificate is an electronic document that is attached to electronic communications, the purpose of which is to prevent its contents from being viewed without prior authorization.

Answer: false Difficulty: 3 Page: 381 Skill Type: applied

6. Newton wants a tool that will allow him to perform one operation: converting plaintext into ciphertext. What he wants is known as decryption software.

Answer: false Difficulty: 2 Page: 382 Skill Type: applied

7. The process used to encrypt electronic documents can also be used to create electronic signatures by reversing the operation of the cryptographic keys.

Answer: true Difficulty: 1 Page: 382 Skill Type: recall

8. Communications security is a combination of information security and computer security.

Answer: false Difficulty: 2 Page: 385 Skill Type: recall

9. Matt Cone has registered the domain name icecreamcone.ca. While Matt plans on using the domain name to promote his homemade ice cream, he is also considering selling the name to the highest bidder and using the money to help offset his start-up costs. Matt has contacted several relevant businesses with his offer. Recently, Matt has received a complaint from a kosher ice-cream distributor that holds a registered Canadian trade-mark for “Ice-Cream Cohen.” It has characterized Matt’s actions as cybersquatting and is demanding that he assign his registration in the domain name to them at cost. Because cybersquatting is an illegal practice, Matt must assign his rights to Cohen.

Answer: false Difficulty: 3 Page: 386 Skill Type: applied

10. Citron Cleaning Supplies has begun marketing their new computer screen cleaner under the name “Compuclean.” Citron is a US-based company and holds a US federally registered trademark for “Compuclean.” Recently, it has discovered that a Canadian company is in the business of vending a similar product through the web site

compuclean.ca. The Canadian website encourages foreign-based orders and maintains an international toll-free phone number for customer inquiries. Instead of bringing a complaint under the domain name arbitration system, Compuclean wishes to bring an action against the Canadian company in a US court. In order to increase the chances that the US court will assert jurisdiction, Citron should argue in favour of the application of a *passive versus active* test.

Answer: true Difficulty: 2 Page: 389 Skill Type: applied

11. Isabella has commenced an action against a Caribbean-based company who offered a “guaranteed seventeen percent return on all 30-day foreign investments of twenty thousand dollars or more.” Both the initial investment and interest were to be repaid in the investor’s national currency, regardless of the mode of investment. Instead, the company provided Isabella with a certificate of ownership in a sugarcane farm, presumably obtained for less than its stated value. Because Isabella is a Canadian citizen she would like the action tried in a Canadian court and, accordingly, must satisfy the *real and substantial connection* test. Under this approach, Isabella must demonstrate that the effects of the Caribbean company (*ie* the harms suffered) were experienced in Canada.

Answer: false Difficulty: 3 Page: 388 Skill Type: applied

12. Hoben Electronic Publishing Co wishes to take proactive steps to insulate itself from potential liability for any libelous content it might inadvertently publish. It has noticed that Southern Ontario is particularly litigious. Accordingly, it has posted a notice on its web site stating that residents of Southern Ontario cannot purchase or download content from the site. These are the only steps taken by the company. Although it had the opportunity to purchase software that would allow it to block access to residents of that region, it has chosen not to do so. Nor has Hoben engaged in further screening at the time of purchase and/or download. Nevertheless, the steps taken by the company are sufficient to avoid liability under the effects-based approach to determining jurisdiction.

Answer: false Difficulty: 2 Page: 389 Skill Type: applied

13. While attending a recent conference on electronic publishing, Samina overheard a colleague remark that online service providers, such as news publishers, can avoid liability against third parties by inserting an exclusion from liability provision in its user agreement, provided that the exclusion clause is sufficiently brought to the attention of its users. The remark that she overheard is incorrect.

Answer: true Difficulty: 2 Page: 391 Skill Type: applied

14. InvestorsTalk.com is in the business of providing a forum so that its customers may post complaints and criticisms regarding the business practices of publicly traded companies. Although InvestorsTalk.com does not monitor its users’ postings, it will occasionally delete particularly reprehensible postings when notified. According to the decision in *Cubby* and *Stratton-Oakmont*, InvestorsTalk.com’s practice of censoring

some messages will insulate the company from liability, regardless of whether it was aware that the illegal messages had been posted.

Answer: false Difficulty: 3 Page: 392 Skill Type: applied

15. A *dot con* is a con artist who makes use of the internet to defraud unsuspecting consumers.

Answer: true Difficulty: 1 Page: 393 Skill Type: recall

### SHORT ESSAY

1. “The *Model Law on Electronic Commerce* is not really a law.” Is this statement true? Explain your answer.

Answer:

The statement is true. Laws are enacted by sovereign nations in order to create rights, powers, obligations, or immunities. The so-called *Model Law on Electronic Commerce* has none of these features. It is more like an international vision, a set of guidelines created by the United Nations Commission on International Trade Law to serve as a model for member states. Its aim is to foster the development of uniform laws across the globe in order to promote international trade in the online environment. Only through an adoption by a legitimate, law making body will these rules have legal effect. Governments may choose to adopt all of or parts of it, at their pleasure.

Difficulty: 2 Page: 375 Type: recall

2. Identify and briefly explain six aspects of Canada’s *Uniform Electronic Commerce Act*. Provide a business law example for each.

Answer:

The six aspects of the *Uniform Electronic Commerce Act* with examples are as follows:

- *Scope*: The *UECA* has a broad scope. Rather than trying to list all the transactions to which it applies, it lists those to which it does *not* apply. Consequently, certain transactions continue to be governed by traditional paper-based rules. For example, the drafting of a person’s last will and testament must, according to the model, be printed on paper and signed in ink in order to be legally enforceable.
- *Consent*: The *UECA* does not prescribe that businesses must accept (or reject) electronic documents. Consent may be either express or implied. Courts will, in some cases, infer consent if business practices would seem to suggest that electronic documents are welcome. For example, a business that sends customers transactional documentation by electronic means may reasonably be expected to accept electronic documents in reply.
- *Functional Equivalents*: A *functional equivalent* identifies the essential purpose of a traditional rule and indicates how that purpose can be accomplished electronically. The *UECA* expressly allows for the use of functional equivalents

with respect to electronic commerce and contracting. For example, clicking an “I AGREE” box or participating in an online interaction may be sufficient to satisfy the traditional pen-and-paper signature that is sometimes required to generate an enforceable contract.

- *Electronic Contracts:* The *UECA* specifically allows for transactions to be achieved by computer programs, with or without human intervention. For example, legally enforceable contracts may be created by preprogrammed shopping bots.
- *Sending and Receiving Electronic Documents:* The *UECA* contains provisions that stipulate where and when a message is sent or received. A message is deemed sent from the sender’s place of business and received at the recipient’s place of business. Also, a message is deemed sent once it leaves the sender’s control and is deemed received when it reaches an information system in the control of the person to whom it is sent. Consequently, a recipient may be found to have received a message regardless of whether it was in fact read. For example, if I reply to your offer on my handheld, wireless email service while on the runway of Pearson International Airport, the email will be said to be sent from Antigonish (my place of business) at whatever time it leaves the control of my information system.
- *Government Documents:* The *UECA* contains provisions regulating electronic documents that are sent to government. Governments may specify the formats that it is willing to accept. For example, a government may refuse to accept certain graphics files, whether or not it has expressly said so.

Difficulty: 2 Page: 376 Type: applied

3. Upon graduation from college, Martine decided to go into the information business. His first venture was a fee-based daily electronic newsletter for online stock traders. Given the time sensitive nature of the information, Martine’s *Terms of Service* promised to deliver the newsletter every business day, no later than 9:00 am Eastern Standard Time. The newsletter was doing fairly well until, one day at 8:42 am EST, Martine spilled Orange Crush on his notebook computer right as he clicked to send the newsletter to the subscriber list. Having experienced a hardware malfunction and having lost a key piece of software and a portion of his address list, the newsletter was sent to some subscribers but not all. Because Martine’s service was down for the rest of the day, those who didn’t receive the newsletter right when it was sent, never did receive the news that day. Martine had no way to determine who received and who did not receive the newsletter. Consequently, several day traders demanded a refund for services not rendered, while others decided to seek damages for lost opportunities. Martine is seeking your advice. Outline the issues involved in this case and advise Martine on how he can prevent future disputes, given the nature of his business.

Answer:

Under prototypical e-commerce legislation, a message is deemed sent from the sender’s place of business and received at the recipient’s place of business. Given his contractual obligation to “deliver the newsletter” by 9:00 am EST, Martine will be more concerned

with the rules regarding *when* a message is sent and received. A message is deemed sent when it leaves the sender's control. On this basis, Martine could legitimately claim that his newsletter was sent at 8:42 am, the very moment he pressed the send button (and the very same moment that the Orange Crush hit the mother board). Alternatively, Martine's subscribers will argue that the applicable rule concerns when the message is deemed received. According to e-commerce legislation, it is deemed received once it reaches an information system in the control of the person to whom it is sent. Martine's subscribers will be deemed to have received the newsletter whether or not they have actually opened and read it, provided that they could have accessed it had they chosen to do so. The difficulty in this case involves a determination of which rule should apply. Martine's contract promised to "deliver the newsletter." Does delivery occur when a message is sent or received? That is the issue up for grabs in this case.

There are a few things that Martine could do to prevent similar future disputes. First, he could change the language in his *Terms of Service*, thereby limiting his obligation to *sending* the newsletter by a certain time. This would have avoided the problem on the facts. But Martine could take further steps. He might, for example, require his subscribers to acknowledge receipt, or he could implement an automated confirmation system. This would not have helped him on the current facts. Another thing Martine could do is remove the obligation to deliver by a certain time altogether. The problem with this last piece of advice is that most of his clients will not subscribe without a guarantee that the newsletter will arrive by a certain time.

Difficulty: 3 Page: 377 Type: applied

4. Many businesses presume that electronic messages that have been sent will be received. Briefly discuss how businesses can proactively prevent the problems that would arise if a message were lost in cyberspace.

Answer:

A lost message can interfere with the parties' ability to achieve a meeting of the minds (*consensus ad idem*). Someone has to bear the burden. When an offer is lost, the worst thing that can happen is that one or both parties miss-out on an opportunity. But when the lost message was meant to communicate acceptance, there is more at stake since one of the parties will believe that there is a contract and will arrange its affairs accordingly, while the other will not. In light of this, prudent risk managers must take extra steps to ensure the successful formation of contracts. First, the offering party should stipulate in the offer when acceptance will be said to occur. (For example, it might stipulate that acceptance occurs only when it is received, rather than when it is sent.) Second, both parties should employ an additional channel of communication (*eg*, fax, regular mail, or telephone) to back up important electronic messages.

Difficulty: 2 Page: 377 Type: recall

5. Contrast and compare *shrinkwrap*, *clickwrap* and *webwrap* licences. Provide an example of each.

Answer:

First, students would do well to note that a *licence* is simply a permission to act in a way that would normally be prohibited, such as using another person’s property. Second, students should answer along the following lines:

- *Shrinkwrap licence*: A shrinkwrap licence is typically used in the sale of mass-market goods, such as software. The licence is physically wrapped between the packaged product and a clear piece of cellophane. The licence states that use of the product constitutes an acceptance of the terms and conditions contained in the licence. The boxes for most proprietary software provide an example.
- *Clickwrap licence*: A clickwrap licence is any licencing arrangement triggered by the click of a mouse. Typically, a clickwrap contract is employed in electronic commerce transactions requiring a consumer to accept the terms of an online contract by clicking a mouse or touching an icon that says “I AGREE.” Some clickwrap licences are instances of a webwrap licence.
- *Webwrap licence*: Webwrap licenses are triggered by some form of online interaction. Often the simple act of viewing a website or downloading software is sufficient to create a valid agreement between the online offeror and consumers. In these cases, the terms and conditions must be easily accessed and understood in order to be enforceable.

In all of the above contracts, a form of interaction is used to express consent and signify *consensus ad idem* in substitution for the traditional pen-and-paper signatures required under contract law. Such devices are referred to as *functional equivalents* on the basis that they satisfy the essential purpose of a traditional rule of contract law.

Difficulty: 2 Page: 378 Type: applied

6. You recently received a notice that your internet service provider has released your personal account information to a third party in connection with a defamation complaint. When you call to contest the service provider’s actions, you are referred to a provision in the terms of service agreement that you apparently did not read (or, at least, you did not remember reading it!). The relevant provision gives permission to release personal information under such circumstances. Can the service provider rely on the provision? Explain your reasoning, using the precedent set out in *Rudder v Microsoft*.

Answer:

Whether the provision is enforceable depends on whether the term is seen as onerous or unusual and whether it was reasonably brought to your attention. According to *Rudder v Microsoft*, clickwrap contracts are a valid form of contracting. Because of their integral role in electronic commerce, consumers may not rely on the fact that they did not read the terms and conditions of a clickwrap contract in order to escape their obligations under the agreement. That said, terms that are not reasonably brought to a person’s attention, *eg*,

those found in a remote hyperlink, or camouflaged in unusual fonts or footnotes, will likely be held unenforceable. The *Rudder* decision requires that the terms and conditions of online agreements be clearly discernible and understood by consumers. Although your service provider probably should have implemented a series of click-through confirmation mechanisms to clearly evidence your agreement to the term, so long as it was brought to your attention, then it will be enforceable—whether you read it or not.

Difficulty: 3 Page: 379 Type: applied

7. Monkey Business Inc has implemented an automated software system that allows its employees to enter their weekly hours. Recently, it was determined that one of its employees made a keystroke error and was underpaid as a result. As a general rule, how can Monkey Business and its employees protect themselves against keystroke errors?

Answer:

According to most provincial electronic commerce legislation, keystroke errors can render a transaction unenforceable, especially when they involve automated systems. Legislation allows a party to escape the consequences of a transaction in which a keystroke error has been committed provided that: (i) the automated system did not provide an opportunity to prevent or correct the error, (ii) the mistaken person notifies the other party of the error as soon as possible, (iii) the mistaken person took reasonable steps to return any benefit received under the transaction, and (iv) the mistaken person did not receive any material benefit from the transaction. Employees can protect themselves by ensuring that the above conditions have been met. Monkey Business can protect itself against keystroke errors by employing automated mechanisms that detect and correct such errors. The simplest solution is to require a party to an electronic agreement to repeat the most important steps or otherwise confirm the details of the transaction.

Difficulty: 2 Page: 380 Type: applied

8. “Cryptography is the science of encryption and decryption.” What is the essential purpose of cryptography? Briefly describe these technologies and provide a business application for each.

Answer:

The essential purpose of cryptography is to create a secure messaging system that prevents access by anyone other than the authorized parties to a transaction. Encryption techniques employ complex algorithms in order to encode the plaintext of a message into an unreadable form called ciphertext. Only those parties in possession of the correct decrypting algorithm can translate the message back into a comprehensible format. Asymmetrical cryptographic systems, such as public key infrastructures, use two distinct keys in order to further ensure the integrity of encrypted messages. A message is encrypted with its recipient’s public key and decrypted with its private key. In this way, a person’s public key is protected against unauthorized use. Encryption and decryption are often used in business to ensure confidentiality. Encryption and decryption technologies



are also used to authenticate electronic signatures or digital certificates created with an employee's private key.

Difficulty: 2 Page: 382 Type: recall

9. Compare *computer security* and *communication security*. Provide two business examples for each. Describe other ways in which a business can seek to protect its information system.

Answer:

*Computer* and *communication* security are both aspects of *information* security.

- *Computer security* Protects information while it is transmitted from one information system to another. Such security utilizes both hardware and software. For example, the cryptographic techniques prescribed by a public key infrastructure may be used to shield the contents of messages in transit. As well, private network lines may be laid down to avoid transmitting confidential information over publicly accessible networks. This is often the case with corporate *intranets*.
- *Communications security* Protects information within a computer system. Again, such security utilizes both hardware and software. For example, anti-virus software should be installed on a business' computer network in order to protect against viral attacks from both within and without. Similarly, external firewalls can be used to erect a screen between a workplace *intranet* and the outside world. Only authorized communications may pass through.

Additionally, businesses can use the law to protect their information systems. Businesses can, to an extent, deter certain security breaches by publishing relevant parts of the *Criminal Code of Canada*. Businesses may further protect themselves through their employment contracts. Finally, businesses may outsource their security needs to third party security providers or insurers.

Difficulty: 2 Page: 385 Type: applied

10. Following a string of unpleasant experiences while eating at a well-known nationally franchised restaurant, you decide to create a web site devoted to making disparaging remarks about it. To increase traffic to your site you select a name similar to that of the restaurant, and register it as a dot-ca with the Canadian Internet Registry Authority. Much to your surprise, the web site quickly gains notoriety after receiving some national mainstream press. Soon, visitors from all over Canada post their own misgivings about the restaurant. You are having great fun with it all until one day when you receive a "cease and desist" order from the restaurant's head office in Winnipeg. Eventually, the restaurant chain files a complaint with an accredited arbitrator under the Canadian Internet Registry Authority's Dispute Resolution Policy. Prepare an outline for your argument. How do you anticipate that the restaurant might respond?

Answer:

As a registered holder of a dot-ca, one will be required to submit to a mandatory arbitration governed by CIRA's Dispute Resolution Policy. The argument I would put forward follows the decision set out in *Wal-Mart Stores, Inc. v wallmartcanadasucks.com and Kenneth J. Harvey*. In that case, the defendant, Harvey, was found to have "a legitimate interest in respect of the domain name, to use it as a foundation for criticism of the complainant." Although I have no commercial rights in the name and will therefore be unable to offset the restaurant's proprietary claim, I do have the right to express myself freely on my own web site. Using the domain name system as a means of preventing my free speech is, in my view, unconstitutional. The restaurant will respond by saying that my argument is a highbrow distraction from the real issue, which is about cybersquatting through a bad faith domain name registration. In particular, the restaurant will argue that my domain name is confusingly similar to their trademark (that is, "the domain name so nearly resembles the mark in appearance, sound or the ideas suggested by the mark as to be likely to be mistaken for the mark"). Moreover, the restaurant might argue that I have registered my domain name in bad faith, in order to disrupt its business.

Difficulty: 2 Page: 386 Type: applied

11. You have recently discovered that your company's domain name, breadandbutter.ca, was registered by a company called Domain Acquisitions Co during a lapse in registration (due to an overlooked outstanding payment). This company has since offered to resell the domain name to your company for a considerable sum. Needless to say you are extremely perturbed. What are your possible courses of action? Decide which remedy you will seek and outline your strategy.

Answer:

As a prudent risk manager you should note the following possible courses of actions and the remedies that they will provide:

- *Arbitration* Because the domain name at issue is a dot-ca, I have the right to file a complaint under the Canadian Internet Registry. By doing so, Domain Acquisitions Co must submit to mandatory arbitration governed by CIRA's Dispute Resolution Policy. Should my company succeed in proving that Domain Acquisitions Co has registered the name in bad faith (that is, specifically registered the domain name in order to resell it for valuable consideration in excess of its actual cost), Domain Acquisitions' registration will be cancelled. I can also ask for the registration to be transferred back to me.
- *Litigation* By choosing to litigate, I would file an action in court alleging trademark infringement by Domain Acquisitions Co. Domain Acquisitions Co would then have the burden of proving that it held a competing commercial right in the name. On the facts, this would seem unlikely. If I am successful, I will likely be able to convince the court to cancel or transfer the registration. However, I can also seek an additional damage award, should the court find the defendant's behaviour to have been injurious.

- *Settlement* Given the time and expense required to seek a remedy through litigation or arbitration, it might be prudent to simply work out a deal at a reasonable price. Such a deal would ideally take into account my own failings in allowing the registration to lapse, as well as the fact that I am likely to be awarded the name should the parties choose to take the matter to court or arbitration.

Given a preference to avoid unnecessary conflict, it might be best to attempt to settle the disagreement without having to resort to formal dispute resolution. However, should the defendant prove unreasonable, my best course of action is likely to submit a complaint to a CIRA accredited arbitrator. This is preferable to litigation, which can take a tremendous amount of time and expense. CIRA accredited arbitration is geared towards providing an inexpensive, quick, and fair resolution to domain names disputes.

[Note to instructors: an answer of this caliber presumes that students have completed the end of chapter research questions]

Difficulty: 3 Page: 387 Type: applied

12. Given the uncertainty involved in determining a company's potential liability in foreign jurisdictions, are there any proactive steps that a company might take to protect itself? Explain your answer and provide examples.

Answer:

One important proactive measure is the use of targeting technologies. Targeting technologies are used in order to specify the locations where you are willing to do business. By restricting the geographical region in which online business can be done, certain jurisdictions can be avoided. Another proactive measure is to insert a jurisdictional clause into any online agreements. Such a provision will require any disputes arising from the transaction to be heard by a particular court, using a particular set of laws. Alternatively, potential customers may be required to consent to an agreement in which the customer is required to: (i) attest that they are not residents of particular jurisdictions, or (ii) agree to indemnify the company in the case that they are being untruthful.

[Student's may also answer this question by discussing the issue of intermediary liability, specifically by contrasting and comparing both distributor and publisher liability. In so doing, they should note that online intermediaries can take steps to design their information infrastructure to serve only a distribution function – that is, the company can avoid exercising editorial control over the content within its network.]

Difficulty: 2 Page: 388 Type: applied

13. You are a manager at a medium sized start-up company that is well positioned in the online intermediary market. One of your colleagues has asked you to offer some advice about the liability of online service providers. Provide a brief introduction to this

issue. Illustrate your answer with business law examples. How can a business shield itself from intermediary liability?

Answer:

As the name suggests, online intermediaries are often the go-betweens in a transaction. Because of the special role that they play in various e-commerce relationships, online intermediaries are exposed to liability in several circumstances. For example, subscribers of an online service might use those services to carry out an illegal act; they might post illegal content to the service provider's web site. Usually, the service provider will be able to determine the identity or other personal information about its subscribers, even if the subscriber commits the illegal act anonymously. If the subscriber does something illegal through the medium of the online services provided, the service provider might be held liable unless it cooperates with the authorities.

In some jurisdictions, a limited number of exemptions have been carved out to allow online service providers to avoid liability on the basis that they are simply providing network access, or in other words, are acting merely as a conduit between the parties to an online interaction. But when service providers go beyond this role and begin taking control over the content, they are more accurately categorized as publishers (rather than distributors) and thereby expose themselves to a greater likelihood of liability. This is certainly true for internet service providers who exercise editorial control over their bulletin boards and newsletters, for example. Moreover, internet service providers may find themselves potentially liable to third parties on account of their customers' actions. Although there is not much that they can do in the case of third party liability, online service providers are advised to set up their services to the greatest extent possible so that they operate as a mere conduit rather than a content provider. Service providers can also shield themselves from liability by way of contract. In order to do so, the terms of service should require subscribers to provide an indemnification in cases where the company is held liable as a result of the subscriber's behaviour.

Difficulty: 2 Page: 390 Type: applied

14. "One common scam (perpetrated by dot cons) involves *multi-level marketing*." Explain the meaning of this statement and indicate whether or not it is true.

Answer:

The statement is true. A dot con is, in essence, a con artist who has gone high-tech, using the internet to defraud costumers. Multi-level marketing is a promotional system that puts more emphasis upon the recruitment of distributors than on the selling of products. This practice is best illustrated as a pyramid scheme in which money gets paid upwards by people lower on the ladder. The monies paid are usually for the initiation fee and product samples and are required in order to join the pyramid. Because most of the money is paid up the ladder, those low on the ladder are unlikely to profit. In this respect, multi-level marketing is a scam aimed at bilking its newest recruits. Although this practice is by no means unique to the internet, it has been successfully implemented online. Other online

dot con scams include: (i) duplicitous auctions, (ii) fraudulent credit card charges, (iii) fictitious business opportunities, and (vii) miracle cures.

Difficulty: 1 Page: 393 Type: recall

15. What are the advantages and disadvantages of a decision by your business to implement Industry Canada's *Principles of Consumer Protection in Electronic Commerce*? Explain your answer.

Answer:

From a legal perspective, there is no advantage or disadvantage to adopting these principles since they do not have the force of law. In other words, their adoption is optional. By implementing these principles into its current practices, a business can enhance its reputation, strengthen consumer confidence, and ultimately increase sales. Publicity and general goodwill can also be leveraged by using the adoption of these principles as an opportunity to showcase a company's commitment to ethical and effective business practices, practices which respect consumer's right to fair treatment and privacy. This should give the business a competitive advantage. However, because these principles may in fact never become law, the cost of their implementation must be weighed against these expected benefits. The adoption of some of the principles will involve significant monetary investment in new technologies, such as installing security mechanisms. The cost of adoption could be too heavy a burden to bear, especially for struggling small to medium sized start-up companies. Nevertheless, common sense dictates that businesses should respect these principles to the extent that the bottom-line allows. Prudent risk managers should realize that, given the likelihood of these principles eventually possessing the force of law, a proactive approach should help them offset investment costs, and gives them an early competitive advantage with those customers sensitive to consumer protection practices.

Difficulty: 1 Page: 395 Type: recall